

UNITED STATES DISTRICT COURT
for the
Southern District of Ohio

United States of America)
v.)
)
) Case No. 2:24-mj-182
Aleksandr Bogomolny)
(aka Alex Bogomolny))
)
)

Defendant(s)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

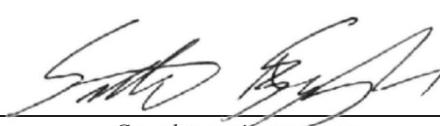
On or about the date(s) of 03/29/2021 to 03/01/2024 in the county of Franklin in the
Southern District of Ohio, the defendant(s) violated:

<i>Code Section</i>	<i>Offense Description</i>
Title 18 U.S.C. § 1956(a)(3)	(money laundering); and
Title 18 U.S.C. § 1956(h)	(conspiracy to commit money laundering).

This criminal complaint is based on these facts:

See attached affidavit incorporated herein by reference.

Continued on the attached sheet.


Complainant's signature

Seth Erlinger, Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Via FaceTime

Date: April 5, 2024

City and state: Columbus, Ohio



**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO
EASTERN DIVISION**

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT

I, Seth Erlinger, a Special Agent (SA) with the Federal Bureau of Investigation (FBI), Columbus Resident Agency, being first duly sworn, hereby depose and state as follows:

1. I, SA Seth Erlinger (your affiant), make this affidavit in support of a criminal complaint to arrest for violations of 18 U.S.C. § 1956(h) – conspiracy to commit money laundering and 18 U.S.C. § 1956(a)(3) – money laundering. Since this affidavit is being submitted for the limited purpose of securing a criminal complaint and arrest warrant, your affiant did not include each and every fact known concerning this investigation. Your affiant did not withhold any information or evidence that would negate probable cause. Your affiant set forth only the facts that are believed to be necessary to establish probable cause that ALEKSANDR “ALEX” BOGOMOLNY (BOGOMOLNY) committed the violations listed above. The FBI believes, as set forth below, BOGOMOLNY has engaged in a conspiracy with, among others, a person this Affidavit will refer to as Coconspirator 1. The true identity of Coconspirator 1 is known to your affiant.
2. I am a SA with the FBI and have been since September 2017. I am currently assigned to the Cincinnati Field Office, Columbus Resident Agency, Cyber Crime Squad, which is responsible for investigating computer and high-technology crimes. During my career as an FBI SA, I have participated in numerous cyber-related investigations. During the investigation of these cases, I have participated in the execution of numerous arrests, search warrants, and seizures of evidence. Since my assignment to the Cyber Crime Squad, I have received both formal and informal training from the FBI regarding cyber investigations. I am trained and authorized to investigate the offenses alleged herein.
3. On or about May 1, 2021, Rogue Fitness (the VICTIM) filed a complaint, via the Internet Crime Complaint Center, regarding unauthorized use of a corporate PayPal account. The VICTIM’s corporate headquarters is in Columbus, Ohio. The account was described by the VICTIM as a generic account, accessible by approximately 90 customer service employees, which would receive and send money transactions daily.
4. According to the VICTIM, between March 29, 2021, and April 29, 2021, approximately 78 outgoing transfers occurred from the VICTIM PayPal account, totaling approximately \$496,136. Each outgoing transfer generated a unique Transaction ID; however, no information was captured to which accounts the money was moved. The VICTIM believed these transactions were fraudulent due to the large sums being transferred and the fact the money was transferred to pre-paid cards instead of bank accounts linked to customers. The VICTIM conducted transactions to customer bank accounts, not pre-paid cards, as normal business activity. The VICTIM was not able to associate the outgoing transfers to any known legitimate transactions of the company.
5. Upon review of a laptop used by a customer service employee working for the VICTIM, the FBI determined the laptop had been infected with a banking Trojan just prior to the

VICTIM experiencing the fraudulent wire transfers. The specific banking Trojan found is known to steal banking credentials and usually targets corporate victims. It is believed the banking Trojan was in fact the cause of the 78 transactions from the VICTIM's PayPal account.

6. On or about June 25, 2021, PayPal provided results to the FBI for account information associated with the 78 Transaction IDs. Results revealed the VICTIM account to be a Business account, in the name of William HENNIGER. According to the VICTIM's website, HENNIGER is the founder of the VICTIM Company. Results from PayPal revealed the money was transferred to approximately 22 different card numbers, one of which was Bank of America card number ending in x7924. The results also showed a transaction of \$19,990 to that card on March 29, 2021, from the VICTIM account.
7. On or about August 13, 2021, Bank of America provided results to the FBI for account information associated with card number ending in x7924. Results revealed the account holder to be BOGOMOLNY, with an address in Brooklyn, NY, and the account type to be checking.
8. Bank of America results for BOGOMOLNY's account showed the following activity, including receipt of the March 29, 2021 transfer from the VICTIM's PayPal account:
 - a. 3/29/21 – deposit of \$19,990.00 from “PayPal #000213177 PMNT RCVD PayPal *Henniger W”
 - b. 3/29/21 – transfer of \$1,400.00 to PERSON A via Zelle. The identity of PERSON A is known to your affiant.
 - c. 3/29/21 – withdrawal of \$1,005.99 from “TNSSMART 2100 Pacific Ave Atlantic City NJ”
 - d. 3/30/21 – transfer of \$1,500.00 to PERSON B via Zelle. The identity of PERSON B is known to your affiant.
 - e. 3/30/21 – withdrawal of \$5,000.00 from checking at “NJ TLR”
 - f. 4/01/21 – transfer of \$2,200.00 to PERSON B via Zelle
 - g. 4/02/21 – withdrawal of \$1,000.00 from “BOA ATM Brighton Beach Brooklyn NY”
 - h. 4/05/21 – withdrawal of \$5,000.00 from checking at “NY TLR”
 - i. 4/05/21 – transfer of \$3,700.00 to checking ending in 0738 via online banking
 - j. 4/06/21 – receipt of \$3,000.00 from checking ending in 0738 via online banking
9. Bank of America also provided images captured during ATM transactions at various bank locations. Two images taken March 26, 2021, and April 2, 2021, showed an

individual that matched the New York driver's license photo of BOGOMOLNY, at a walk-up ATM located approximately 0.5 miles from BOGOMOLNY's residence. These images were taken a few days prior to and after BOGOMOLNY received the funds from the VICTIM's PayPal account.

10. On August 4, 2022, pursuant to a judicially authorized search warrant issued by the United States District Court for the Eastern District of New York on August 3, 2022, the FBI executed a search of BOGOMOLNY's residence.
11. During the execution of the search warrant, BOGOMOLNY was interviewed and provided the following statements:
 - a. BOGOMOLNY would not receive money into his own personal bank account from individuals he did not know.
 - b. BOGOMOLNY did not recognize or know HENNIGER's name, even though \$19,990 had been deposited into BOGOMOLNY's personal bank account from HENNIGER's account.
 - c. BOGOMOLNY was provided with the below chart showing a summary of deposits and withdrawals from his Bank of America account between December 2019 and July 2021. When asked what each month's movement of money looked like, BOGOMOLNY responded with "money laundering."

DATE RANGE	DEPOSIT	WITHDRAWAL/ TRANSFER
12/14/19 - 01/15/20	\$5,756.26	\$5,748.43
01/16/20 - 02/12/20	\$3,113.21	\$2,999.04
02/13/20 - 03/16/20	\$1,017.09	\$1,000.00
03/17/20 - 04/15/20	\$11,251.29	\$11,200.01
04/16/20 - 05/13/20	\$24,980.08	\$24,874.00
05/14/20 - 06/15/20	\$21,051.27	\$21,009.00
06/16/20 - 07/16/20	\$24,134.18	\$24,200.00
07/17/20 - 08/14/20	\$22,289.85	\$22,125.00
08/15/20 - 09/15/20	\$41,588.98	\$36,740.84
09/16/20 - 10/15/20	\$9,755.37	\$14,621.42
10/16/20 - 11/12/20	\$4,063.20	\$4,165.04
11/13/20 - 12/15/20	\$5,912.69	\$5,777.62
12/16/20 - 01/13/21	\$4,632.76	\$4,663.46
01/14/21 - 02/10/21	\$2,059.76	\$55.85
02/11/21 - 03/16/21	\$6,748.13	\$8,062.07
03/17/21 - 04/15/21	\$33,121.34	\$33,771.20

04/16/21 – 05/13/21	\$17,961.34	\$17,988.06
05/14/21 – 06/15/21	\$6,545.44	\$6,545.18
06/16/21 – 07/15/21	\$1,635.67	\$1,567.69

- d. According to BOGOMOLNY, he had received an email from an unknown individual in 2020 to his email account regarding an opportunity to make money. BOGOMOLNY thought the email came from some type of company name, but could not recall. BOGOMOLNY filled out an application. The unknown individual advised BOGOMOLNY of the money being deposited into his account, then directed BOGOMOLNY to withdraw and send via Bitcoin to wallets provided by the unknown individual. BOGOMOLNY was supposed to keep 10% of the money deposited into his account. The unknown individual told BOGOMOLNY the money was for his business and that it was all “legit.” In 2021, the unknown individual stopped communicating with BOGOMOLNY.
12. During the review of the electronic evidence seized from BOGOMOLNY’s residence, the following was found:
- a. An Excel spreadsheet named “ssn1” containing approximately 341,761 unique identifiers (First Name, Last Name, Address, Date of Birth, and Social Security Number);
 - b. Photo displaying the front of Arizona Drivers License in the name of a specific individual, with date of birth and home address;
 - c. Photo displaying the front of New Jersey Drivers License in the name of another specific individual, with date of birth and home address;
 - d. Photo displaying the front of New York Drivers License in the name of another specific individual, with date of birth and home address;
 - e. A text document named “List” containing approximately 10 full credit card numbers with expiration, cvv, and zip code; 4 bank accounts with routing numbers; 249 gift/reward cards, with full number and PIN, ranging in amounts from \$5 to \$250;
 - f. Photos of cellphone screens displaying VISA Cash Cards with full number, cvv, expiration date, in the names of another three specific individuals;
 - g. Photo of U.S. passport in the name of another specific individual, as well as a photo of the back of a Bank of America card in the same name, with full card number, cvv, and expiration date;
 - h. Photo of a cellphone screen displaying an online gambling account in the name of PERSON C, whose identity is known to your affiant, on April 27, 2022, with a playable balance of \$1,245.03;

- i. A password stored in a browser for the site Verified.sc, a site known to the FBI to market and traffic information such as credit card and identity data.
13. A confidential source told the FBI they met Coconspirator 1 in Atlantic City, New Jersey some time in 2021. The source and Coconspirator 1 socialized in the lounges of Atlantic City, and the source created a FanDuel account at Coconspirator 1's direction. The source controlled the account for a short time, before Coconspirator 1 took over the account and changed the password. Additionally, Coconspirator 1 would direct the source to go to a casino, such as the Golden Nugget in Atlantic City, where the source could cash out their FanDuel account. Coconspirator 1 would then direct the source as to how to split up the money, with some going to BOGOMOLNY, some to Coconspirator 1, and then a small fee to be kept by the source. The confidential source was not facing criminal charges at the time they provided information to the FBI. The confidential source received money from the FBI in exchange for providing information.
14. For example, on April 20, 2022, Coconspirator 1 sent the source a photo of a card with the name Dickie Armand, a card number ending in x3180, along with the card verification value (CVV) and expiration date. Coconspirator 1 then directed the source "Deposit \$101, \$199" into the source's FanDuel account.
15. On April 21, 2022, Coconspirator 1 told the source "So, look, I have invested \$1200 into your account. Any money we make, I am gonna deduct \$1200 and remaining funds 1/4 is yours" and then "we have just requested \$1400 cage withdrawal. And it should be ready in 1-2 hour for pick up. So you will need to go and pick up money, $\$1400 - \$1200 = \$200 / 4 = \50 is yours so far. And any withdrawal after this you will get 1/4." Later, Coconspirator 1 further detailed the breakdown, stating "From this \$580, \$145 is yours and \$435 is mine. So you put \$435 in to your account and send Zelle to me. And from previous \$1400, you take \$50 and give Alex \$1350."
16. In an interview with the FBI in November 2023, Dickie Armand stated in November 2022 his account at First Horizon was compromised, and about \$4,900 was taken out of the account over the course of approximately 77 CashApp transactions. Armand believed all the transactions were in different names, and Armand did not know any of the people. Additionally, Armand never played any online gambling, including FanDuel, and had never been to Atlantic City.
17. Similarly, in August 2022, Coconspirator 1 sent the source photos of cards with the names Bush AAngela (x1083), Mishell Abarca (x2188), Nicole Yardley (x4188), Alisa Hageon (x3482), Maleatha Tarver (x0643), Robin Gomez (x8886), Morales Aaron (x0924), Leah Abad (x1241), and Mirian Abad (x4143). Each time Coconspirator 1 sent a photo of a card to the source, he also provided directions to the source on how much to deposit into the FanDuel account.
18. The Social Security numbers for Dickie Armand, Bush AAngela, Mishell Abarca, Nicole Yardley, Alisa Hageon, Maleatha Tarver, Robin Gomez, Aaron Morales, Leah Abad, and Mirian Abad were all found in the "ssn1" spreadsheet recovered from BOGOMOLNY's device referenced in paragraph 12(a).

19. The FBI determined the above cards sent by Coconspirator 1 to the source were all related to CashApp accounts. The FBI reviewed account details and determined the accounts were connected by registration or device activity.
 - a. For example, the accounts registered in the names of Armand, Tarver, and Yardley used BOGMOLNY's alexaist17@aol.com email address, which BOGMOLNY also used to register his player account with the Tropicana Casino.
 - b. The accounts registered in the names of Tarver, Yardley, Abarca, Gomez, and Leah Abad all used the address 8200 Boulevard East, North Bergen, NJ 07047.
 - c. Additionally, the accounts registered in the names of Leah Abad, Gomez, and Bush all shared a device ID, indicating they had been created or accessed from the same device.
 - d. Moreover, IP address data for the CashApp accounts in the names of Armand, Morales, Tarver, Mirian Abad, Mceachern, and Hageon indicated each was accessed from a device with a time zone set to either Tashkent or Samarkand, Uzbekistan. Coconspirator 1 is a national of Uzbekistan.
 - e. The accounts in the names of Armand, Tarver, Mceachern, and Hageon all had peer-to-peer transfers with an account held in Coconspirator 1's name.
20. The CashApp account registered in Tarver's name was one of approximately 18 CashApp accounts that cumulatively made deposits totaling approximately \$11,779 into a FanDuel account in the name of Christopher Kinder. The same FanDuel account had deposits from Sightline totaling approximately \$190,355. Sightline is a mobile payments solution provider used by FanDuel, among other online gaming platforms.
21. The same FanDuel account held in the name of Christopher Kinder had approximately \$186,341 in withdrawals. The withdrawals were primarily completed via ACH transfers to a Chime spending account ending in x0249, in addition to over-the-counter withdrawals and a PayPal account registered with email kinder99pa@mail.com.
22. Additionally, the Kinder FanDuel account received funds from two Bancorp Bank cards, which were tied to a Bancorp Bank account in Kinder's name. This account in turn received ACH transfers from individual Bank of America accounts held in Coconspirator 1's and BOGMOLNY's names.
23. In a February 2024 interview with the FBI, Kinder stated that he tried FanDuel one time in 2021, but could not get it to work. Kinder later got a FanDuel bill for about \$250 and had collectors after him to pay it. Kinder did not understand how he could be billed by FanDuel when he never put money in or made any bets. Kinder stated he lost his wallet during a trip to Atlantic City in July 2021.
24. Similar to the account held in Christopher Kinder's name, the FBI has identified at least two other FanDuel accounts held in the names of individuals who have provided

information to the FBI. Based on the information provided to the FBI, your affiant believes these individuals opened the accounts and then provided BOGOMOLNY and/or Coconspirator 1 with the user credentials, after which Coconspirator 1 and/or BOGOMOLNY exercised control over the accounts. The first account had approximately \$161,790 in deposits and approximately \$121,350 in withdrawals. The second account had approximately \$200,584 in deposits and approximately \$177,854 in withdrawals, including to a PayPal account using the email address dansterjon@gmail.com.

25. Coconspirator 1 previously used email address dansterjon@gmail.com to register a FanDuel account under his own name in April 2021.
26. Thus, between Kinder's FanDuel account and the two FanDuel accounts described in paragraph 24, there were approximately \$571,829.90 in deposits and approximately \$485,545 in withdrawals.
27. In 2023, undercover FBI agents made contact with BOGOMOLNY. In a meeting with undercover FBI agents in October 2023, BOGOMOLNY made the following statements, which were audio recorded:
 - "Okay look, let me tell you story. What happened was, when it was pandemic time, I moved to the Florida. I was living in Fort Lauderdale, in the boat."
 - "I was dealing with bitcoins. Moved my own, boom, boom (inaudible) transaction (inaudible)"
 - "And last transaction was, somebody stole money, and gave me two-hundred fifty thousand Euros."
 - "And I was buying bitcoin. And after two years, FBI came to my house."
 - "They were doing search. They tried to find the program who was inject into the business and steal all the money. They confiscate all my shit, ten laptops, five phones, all kinds of stuff."
 - "Okay, they came to me, 5 (inaudible), August 4, last year, search my house, for the weapons, for the all kind of shit. I have a chair, and under chair, I have a cache, two hundred thousand. This motherfucker can't find."
 - "Can you imagine? And I have some devices, like a flash drives, all kinds of shit."
28. In a second meeting with undercover FBI agents in November 2023, BOGOMOLNY agreed in a recorded conversation to launder \$20,000 of cash for the agents for a 6% fee. The funds were represented by the undercover agents as proceeds of illegal drug activities and BOGOMOLNY understood the request from the undercover agents was for the agents to receive "clean" and "legitimate" money back from BOGOMOLNY.
29. BOGOMOLNY discussed with the undercover agents his prior experience laundering money, including using "business accounts", "wire international", "doing ACH"

transfers, “casinos” and “CashApp”. BOGOMOLNY stated he would “talk to my people” about how exactly to launder the money, whom he later identified by using a first name. This first name was the same as the first name of Coconspirator 1.

30. In the same November 2023 meeting in a conversation with an undercover FBI agent, BOGOMOLNY stated:

- a. Alex Bogomolny (AB): “...because I didn’t know they send me stolen money. You know?”

Undercover (UC): “You didn’t even know you were doing that?”

AB: “No. I was just selling bitcoin.”

UC: “How’d they find you? Like, how did they...find you to buy it, or to, buy the bitcoin from?”

AB: “This guy sent, sent money into my business account”

UC: “Well, I mean, how did they find you?”

AB: “Who?”

UC: “Whoever these people that fucked you or-“

AB: “Oh, from the, from the forum.”

UC: “Oh, you were on a...”

AB: “Hack-, hacking forum.”

UC: “A hacking forum, I got you.”

AB: “Yeah. That means, I wanna buy these coins. I said, I have it. And they send me bad money, you know?”

31. In a text message exchange with an undercover agent on November 9, 2023, BOGOMOLNY used the first name of Coconspirator 1 to describe a person who wanted to use bank transfers to launder the money, and stated “We will set up different casinos accounts”. In the same conversation, the undercover agent asked BOGMOLNY “How much can you put on the debit card at one time?” to which BOGMOLNY replied “9” and later “No irs...That’s why 9”. It is your affiant’s understanding that this refers to the legal requirement that bank representatives must fill out a Currency Transaction Report whenever a customer conducts a currency transaction of more than \$10,000. Some individuals conduct transactions at or below \$10,000 (such as \$9,000, or “9” in the text message exchange) to evade the reporting requirement.

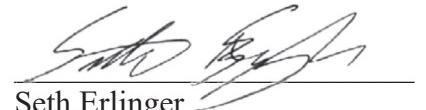
32. On November 20, 2023, in the same text exchange, BOGOMOLNY further explained to the undercover agent that “fresh” casino accounts had deposit limits, which slowed his

progress in laundering the funds. As an example of what could be accomplished with an established account, BOGOMOLNY sent a screenshot of a FanDuel account created on or about February 11, 2022, showing total winnings of \$883,072.28.

33. On November 30, 2023, BOGOMOLNY told the undercover agent he had created a business entity, Massages By Ashley, and was “Going to open a business account”. The following day, December 1, 2023, BOGOMOLNY stated “We have three accounts FanDuel. We will finish with your deposit soon. Waiting for bank approval too.”
34. On December 4, 2023, BOGOMOLNY sent the undercover agent a screenshot of a FanDuel account, created on or about July 16, 2021, showing total winnings of \$2,786,797.39, and the comments “We have had that account for a long time” and “On this account we are making 100k for the week.”
35. On December 6, 2023, the undercover agent inquired via text message as to when the balance of the laundered funds would arrive in their account. BOGOMOLNY replied “We work on it. We are doing software upgrades. I think they hire a fresh IT support team.” Later, BOGOMOLNY wrote “We have a big team” and “BlackSnake Team”.
36. On December 7, 2023, BOGOMOLNY wrote to the undercover agent “We got new software, checking all day. Run good” He also wrote, “It’s going to be faster and more productive”. He also wrote, “They can see that worm”. When asked to clarify, BOGOMOLNY said “We were hijacking with my Killnet team. We have a control system right now.” When asked whether it would be harder for them, meaning FanDuel, to see, BOGOMOLNY replied “If they see, I am going to put encryption for that database. Until they pay me.” BOGOMOLNY stated they had set up three FanDuel accounts and had two people working “for your account”.
37. On December 11, 2023, BOGOMOLNY added the undercover agent to a chat with Coconspirator 1. During the chat, Coconspirator 1 stated “we are able to withdraw around \$8k per day 5 times a week” and “So weekly, we can withdraw \$40k”. The undercover agent replied “We’re open to ideas, we just need it clean” to which BOGOMOLNY responded with a sunglasses smiley emoji. Coconspirator 1 then stated “Our limit is fixed. So if \$200k then it will take 2 month”. The undercover then inquired “Ok, do you have any other operations that would move our money and back to us to clean?” Coconspirator 1 replied, “Yeah, we can do \$20k per day”. Later, Coconspirator 1 stated “It takes me 5 days to move money clean and good brother. But I ask 2 weeks just in case.”
38. Between November 2023 and March 2024, BOGOMOLNY sent \$18,800 of the original \$20,000 back in multiple ACH transactions to an FBI-controlled account, administered by an undercover agent in the Southern District of Ohio.
39. In follow-on conversations with an undercover FBI agent located in the Southern District of Ohio, BOGMOLNY agreed to another meeting in order to receive an additional \$50,000 to launder for the undercover agents.

40. In addition, according to a CBS Miami article, in or around August 2013, BOGOMOLNY was arrested by Immigration and Customs Enforcement while he waited in the New York JFK airport for a flight to Russia. The Monroe County Sheriff's Office in Florida had been investigating BOGOMOLNY after he was found to have had a number of credit cards with different names found on his person. The investigation determined BOGOMOLNY opened credit accounts under other people's names. It was believed BOGOMOLNY flew out of Key West to New York and was attempting to leave the country. The news story is available at <https://www.cbsnews.com/miami/news/keys-man-wanted-for-credit-card-fraud-busted-on-his-way-to-russia/>.
41. Per Monroe County Florida Court case number 13-CF-000579-A-K, on or about December 17, 2013, BOGOMOLNY pleaded guilty to two counts of Fraudulent Use of Personal Identification, one count of Dealing in Credit Cards of Another, and one count of Traffic in Counterfeit Credit Cards. BOGOMOLNY was sentenced to 180 days in jail, two years of community control, one year of probation, court costs, fines, and a requirement to surrender his passport.
42. Based upon the foregoing, your affiant submits there is probable cause to believe ALEKSANDR BOGOMOLNY has violated of 18 U.S.C. § 1956(h) – conspiracy to commit money laundering and 18 U.S.C. § 1956(a)(3) – money laundering. Therefore, your affiant respectfully requests this court issue a criminal complaint and arrest warrant.

Respectfully submitted,



Seth Erlinger
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on April 5, 2024

